

1 DUANE MORRIS LLP  
Karineh Khachatourian (CA SBN 202634)  
2 kkhachatourian@duanemorris.com  
Patrick S. Salceda (CA SBN 247978)  
3 psalceda@duanemorris.com  
David T. Xue, Ph.D. (CA SBN 256668)  
4 dtxue@duanemorris.com  
2745 Hanover Street  
5 Palo Alto, CA 94304-1194  
Telephone: 650.847.4150  
6 Facsimile: 650.847.4151

7 Attorneys for Plaintiff  
NETAPP, INC.

9 **UNITED STATES DISTRICT COURT**  
10 **NORTHERN DISTRICT OF CALIFORNIA**  
11 **SAN JOSE DIVISION**

12 NETAPP, INC.,

13 Plaintiff,

14 v.

15 NIMBLE STORAGE, INC., MICHAEL  
16 REYNOLDS, an individual, and Does 1-50  
17 Defendants.

Case No. 5:13-cv-05058-LHK

**SECOND AMENDED COMPLAINT FOR  
VIOLATION OF THE COMPUTER  
FRAUD AND ABUSE ACT (18 U.S.C.  
§ 1030); TRESPASS TO CHATTEL;  
BREACH OF CONTRACT; UNFAIR  
COMPETITION**

**DEMAND FOR JURY TRIAL**

1 Plaintiff NetApp, Inc. (“NetApp” or “Plaintiff”), by its attorneys, alleges as follows:

2 **NATURE OF THE ACTION**

3 1. Defendant Nimble Storage, Inc. (“Nimble”) is a company built on NetApp’s  
4 innovation. Nimble has engaged in unlawful hiring and business practices in order to rapidly bring  
5 to market products that it could not have created but for its reliance on NetApp. Nimble has publicly  
6 declared that it is the Silicon Valley-based data storage specialist with the record of being the fastest  
7 growing data storage company in history. Nimble’s self-proclaimed growth is due to its illegal  
8 conduct. Throughout its existence, Nimble has targeted and encouraged NetApp employees and  
9 resellers worldwide to join the company and to take NetApp’s confidential and non-confidential  
10 information with them in violation of their contractual obligations. Some former NetApp employees  
11 and resellers did just that, and now Nimble is using that illegally-acquired information to compete  
12 unfairly against NetApp in the marketplace. Upon information and belief, Nimble also has directed  
13 former NetApp employees in Australia, prior to them leaving NetApp, to delete and/or render  
14 unrecoverable, inaccessible, or unavailable NetApp information stored on their workstations to  
15 further frustrate NetApp’s ability to compete in the marketplace.

16 2. NetApp attempted to resolve this dispute with Nimble before filing suit, but all  
17 efforts at resolution failed. NetApp now brings this action for injunctive relief and damages against  
18 Nimble and Michael Reynolds (“Reynolds”) for violation of the Computer Fraud and Abuse Act,  
19 18 U.S.C. §§ 1030 *et seq.*, trespass to chattel, breach of contract, and unfair competition.

20 **THE PARTIES**

21 3. NetApp is a Delaware corporation with its principal place of business at 495 East  
22 Java Drive, Sunnyvale, California 94089.

23 4. Nimble is a Delaware corporation with its principal place of business at 211 River  
24 Oaks Parkway, San Jose, California 95134.

25 5. Upon information and belief, Defendant Reynolds is a citizen of Australia, and  
26 resides in Melbourne, Australia. Upon further information and belief, Reynolds is a Systems  
27 Engineer with Nimble in its Australian sales office.

28 6. To attempt to avoid liability in this lawsuit, both Nimble and Reynolds maintain that

Reynolds is employed by Nimble Storage Australia Pty Limited (“Nimble AUS”), Nimble’s Australian “affiliate.” If Nimble AUS is a separate legal entity and not a sales office, there exists, and at all relevant times existed, a unity of interest and ownership between Nimble and Nimble AUS such that any individuality and separateness between them has ceased, and Nimble is the alter ego of Nimble AUS where Nimble AUS is a mere shell and instrumentality of Nimble as a conduit for a single venture. Upon information and belief, Nimble has been exercising strict supervision, control, and dominion over Nimble AUS’ activities, decisions, policies, and practices related to sales goals, sales tactics, compliance, regulatory affairs, medical affairs, research and development, human resources, legal issues, budgeting, accounting, employee compensation, employee benefits, employee expenses, manufacturing, and public relations at least because: (a) Nimble has been controlling the business and daily operations of Nimble AUS, the Australian proprietary company controlled by Nimble pursuant to Australia Corporations Act 2001, § 50AA; (b) Nimble AUS’ regulatory filings declare that it is 100% owned by Nimble, which it identifies as its “Ultimate Holding Company” – e.g. wholly owned subsidiary; (c) Nimble is identified as the sole member of Nimble AUS, and Suresh Vasudevan (Nimble’s Chief Executive Officer), Anup Singh (Nimble’s Chief Financial Officer) and David Chung (Nimble’s VP Corporate Controller), all executives of Nimble are listed as Nimble AUS’ directors; (d) Nimble’s own regulatory filings in the United States, including its most recent Annual Report (10-K) filed on April 17, 2014, refer to Nimble’s Australian operations as a “sales office;” (e) Nimble boasts in press releases that it has “employees” in Australia; (f) Nimble handles the administration of Nimble AUS including the recruitment, hiring, legal defense, insurance and discipline of employees for “Nimble AUS;” (g) Nimble and not “Nimble AUS” is paying for Reynolds’ attorneys’ fees in this action and is controlling the defense; (h) contracts are made in the name of Nimble and not Nimble AUS; (i) Nimble AUS does not pay taxes for conducting business in Australia because it is controlled by Nimble; (j) Nimble AUS does not have separate email or company website apart from Nimble; (k) Nimble issues all press releases on behalf of Nimble AUS; and (l) Nimble recognizes Nimble AUS’ revenue as its own as stated in its corporate filings including its most recent Annual Report (10-K) filed on April 17, 2014.

7. Adherence to the fiction of the separate existence of Nimble as an entity distinct from

1 Nimble AUS would permit an abuse of the corporate privilege and would sanction fraud and  
2 promote injustice at least because: (a) NetApp is informed and believes that Nimble has been  
3 controlling Nimble AUS' budget, has had to approve all significant spending at Nimble AUS, has  
4 recognized Nimble AUS' revenue as its own, has allotted specific amounts for Nimble AUS to spend,  
5 and is responsible to pay Nimble AUS' liabilities; (b) until this lawsuit, Nimble has never claimed  
6 that Nimble AUS is a separate entity and has said the opposite in press releases and its public  
7 corporate filings; and (c) Nimble is attempting to avoid liability for acts that occurred in California  
8 by now hiding behind Nimble AUS.

9 8. NetApp is unaware of the true names and capacities of Does 1 through 50, inclusive,  
10 whether individual, partnership, corporation, unincorporated association, or otherwise, and therefore  
11 sues these defendants under such fictitious names. NetApp will amend its Complaint to allege their  
12 true names and capacities when ascertained.

13 9. Upon information and belief, at all times herein mentioned, each Defendant acted  
14 individually and/or as the agent, co-conspirator, aider, abettor, joint venturer, alter ego, third-party  
15 beneficiary, employee, officer, director, or representative of Nimble and, in doing the things  
16 hereinafter averred, acted within the course and scope of such agency, employment, or conspiracy  
17 and with the consent, permission, and authorization of Nimble. Upon information and belief, all  
18 actions of each Defendant as averred in the claims for relief stated herein were ratified and approved  
19 by Nimble, or its officers, directors, or managing agents.

#### 20 **JURISDICTION AND VENUE**

21 10. This Court has subject matter jurisdiction over this action pursuant to the Computer  
22 Fraud and Abuse Act, 18 U.S.C. §§ 1030 *et seq.*

23 11. This Court has personal jurisdiction over Nimble because it maintains its principal  
24 place of business within the Northern District of California and because it harmed NetApp in this  
25 district by seeking a competitive advantage through, among other things: (1) wrongful use of  
26 NetApp's confidential and proprietary information obtained by NetApp's former employees; (2)  
27 upon information and belief, directing former NetApp employees to take, delete, and/or withhold  
28 NetApp's confidential and proprietary information, to the detriment of NetApp and for the benefit of

1 Nimble; and (3) upon information and belief, directing Reynolds to access NetApp's protected  
2 databases to the detriment of NetApp and for the benefit of Nimble. Reynolds' acts as alleged herein  
3 were directed by Nimble by itself or as the alter ego of Nimble AUS such that it could reap the  
4 benefits of innovation created and fostered by NetApp over decades and at great expense.

5 12. This Court has personal jurisdiction over Reynolds because he intentionally accessed,  
6 without authorization and/or exceeding authorization, NetApp's protected computer, which he was  
7 advised resides in the forum state (California), and which he knew would cause (and did cause)  
8 harm to NetApp, a resident of California. Reynolds' initial access to NetApp's protected computer  
9 was administered by NetApp in California via a username and password pair. Reynolds also  
10 registered on NetApp's Support Portal to gain access to NetApp training courses, as well as other  
11 resources, software, and materials, with notice that these items are connected to California. For  
12 example, Reynolds also agreed to the terms of the NetApp data protection authorization policy  
13 during the Support Portal registration process, which states clearly that the NetApp global system  
14 database – on which his and other users' personal data resides – is located in Sunnyvale, California,  
15 U.S.A. Further, the user manual for the Synergy database, one of the databases which Reynolds  
16 improperly accessed, denotes that it was prepared by NetApp in Sunnyvale, California, and contains  
17 confidential and proprietary information belonging to NetApp. Moreover, upon information and  
18 belief, Reynolds has attended meetings at Nimble headquarters in San Jose, California, in person,  
19 via videoconference, by telephone, or other electronic or virtual means, and communicates with  
20 Nimble personnel located in San Jose, California via telephone, fax, email, and mail. On further  
21 information and belief, Reynolds communicated with Nimble's headquarters in San Jose, California  
22 during his hiring process. And further still, the End User License Agreement ("EULA") between  
23 Reynolds and NetApp, which is one basis for NetApp's breach of contract claim against Reynolds,  
24 is deemed to have been made in and is construed pursuant to the laws of the State of California.  
25 Accordingly, Reynolds has purposefully directed his activities to the State of California and/or  
26 purposefully availed himself of this jurisdiction.

27 13. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b) because, *inter alia*, a  
28 substantial part of the events and omissions giving rise to the claims occurred here and because

defendants are subject to personal jurisdiction in this district.

### **INTRADISTRICT ASSIGNMENT**

14. Division assignment to the San Jose Division of the United States District Court for the Northern District of California is proper pursuant to Civil Local Rule 3-2(e) because a substantial part of the events giving rise to the claims occurred in Santa Clara County, California.

### **FACTUAL ALLEGATIONS**

#### **A. Through Work and Investment, NetApp Becomes an Innovator and Market Leader**

15. Founded in 1992, NetApp is a Fortune 500 storage and data management solutions provider with a focus on continued innovation to meet its customers' evolving business needs. The company shares a vision of being a model company where it delivers the best possible results for the communities it serves by living a set of core values that includes winning in the marketplace with integrity and honor. NetApp believes that a great culture is the foundation for such success, and it practices what it preaches. NetApp consistently is recognized by the Great Place to Work Institute, *Fortune* magazine, and other local publications as a great place to work in countries and cities around the world. In 2012, NetApp ranked among the top 10 Great Places to Work in all 20 of the locations around the world where it participated in Best Workplace rankings and currently is ranked sixth in the United States. In October 2013, NetApp was recognized by the Great Place to Work Institute as the #3 "World's Best Multinational Workplace."

16. Over the past 21 years, there has been a massive explosion in the use and retention of electronic data as a result of many factors including the rise of the Internet, e-commerce, online banking, electronic mail, the migration from largely paper record keeping to nearly exclusive electronic record retention, enterprise-level desktop virtualization, and the cloud, to name a few. Throughout this time, NetApp has continued to enable customers to store, manage, and protect their electronic data with a wide variety of innovative products, technologies, and solutions that have helped transform the data storage industry.

17. In addition to the factors noted above, the increased usage of email and database systems for real-time e-commerce applications has created significant strain on organizations' ability to effectively and efficiently store and manage their electronic data. Both types of applications

1 dramatically increased the amount of data records that organizations must retain for each employee  
2 and/or customer.

3 18. NetApp has delivered key innovations during this period that enable organizations to  
4 more efficiently address their burgeoning storage requirements without sacrificing data integrity or  
5 security. To remain a leader in the industry it helped create, NetApp devotes tremendous resources  
6 to the development of new technologies and processes. In 2012 alone, NetApp's research and  
7 development expenditures exceeded \$900 million. NetApp also has been widely acclaimed for its  
8 spirit of innovation, including recognition from *Forbes* as one of the "World's Most Innovative  
9 Companies," by *Intellectual Property Owners Association* as a "Top 300" United States patent  
10 holder, and by *IEEE Spectrum* as the best "Quality Over Quantity" patent portfolio in its industry.

11 19. NetApp's research and development investments are of paramount importance  
12 because the markets in which it competes are subject to rapid technological change, evolving  
13 standards, changes in customer requirements, and new product introductions and enhancements. As  
14 a result, NetApp's success depends in significant part upon its ability, on a cost-effective and timely  
15 basis, to continue to enhance its existing products, develop and introduce new products that improve  
16 performance and functionality, reduce total cost of ownership, and deliver high quality products and  
17 services.

18 20. Given the competitive world of high technology, where innovation is the bedrock of  
19 success, NetApp's confidential and proprietary information is among its most valuable assets  
20 because it allows the company to provide sophisticated software and hardware products and services  
21 to satisfy the high standards of performance and reliability required by its customers. If NetApp's  
22 proprietary and confidential information is misused, a competitor may gain an unfair advantage even  
23 though it did not invest the time, money, and/or other resources that NetApp did to develop such  
24 products, services, and technologies. To prevent against such wrongdoing, NetApp protects its  
25 proprietary and confidential information with various data protection techniques including secure  
26 logins and passwords.

27 ///

28 ///

1 **B. Nimble Raids NetApp By Recruiting Its Employees and Obtaining NetApp's**  
2 **Information To Start an Australian Sales Office To Compete Unfairly In the**  
3 **Marketplace**

4 21. NetApp and Nimble are direct competitors in the highly competitive data storage  
5 industry. Unlike other startup companies, which often launch an initial product and subsequently  
6 evolve that product based on customer feedback, Nimble has achieved rapid growth and customer  
7 adoption because, in the words of its CEO Suresh Vasudevan ("Vasudevan"), a former NetApp  
8 executive, Nimble "quickly established parity on a range of features that are typically only to be  
9 found in mature products that have been around for a decade or so." This feat was not accomplished  
10 by starting from scratch. Rather, Nimble needed to rely heavily on foundational information as to  
11 the internal working of NetApp's products and its proprietary business processes. Nimble obtained  
12 this information and know-how by directly targeting NetApp employees and resellers and  
13 encouraging them to bring NetApp's proprietary information and other NetApp property with them  
14 such that Nimble could rapidly bring to market storage systems to compete with NetApp.

15 22. Vasudevan also has been quoted as saying that "In just two and a half years of  
16 shipping product, we have an installed base of over 1,100 customers and over 2,000 deployments."  
17 Nimble could not have developed its business so rapidly but for its improper and illegal use of  
18 NetApp innovation. NetApp's products are the result of decades of hard work, including billions of  
19 dollars in research and development expenditures.

20 23. Nimble has identified hiring and expanding its sales force as key factors in its ability  
21 to be successful. Nimble acknowledged in its recent Form S-1 filing with the United States  
22 Securities and Exchange Commission ("S-1") that hiring in the San Francisco Bay area is  
23 competitive and that in the past it has experienced difficulty in hiring and retaining highly skilled  
24 employees with appropriate qualifications.

25 24. Nimble further explained in its most recent Annual Report (10-K) filed on April 17,  
26 2014 that one of its challenges is expanding internationally and, specifically in Australia, recruiting  
27 and retaining the "right" personnel. Nimble advised that "many of our existing competitors have,  
28 and some of our potential competitors could have, substantial competitive advantages such as ...

1 larger sales and marketing and customer support budgets and resources [and] broader distribution  
2 and established relationships with distribution partners and end-customers. Our future growth plan  
3 depends in part on expanding outside of the United States.” Nimble continued:

4 As part of our growth plan, we intend to expand our operations globally.  
5 We have a limited history of marketing, selling and supporting our  
6 products and services internationally. International sales and operations  
7 are subject to a number of risks, including the following: ... difficulties in  
8 attracting and retaining personnel with experience in international  
9 operation[.] These factors and other factors could harm our ability to gain  
10 future international revenue and, consequently, materially impact our  
11 business and operating results. The expansion of our existing international  
12 operations and entry into additional international markets will require  
13 significant management attention and financial resources. Our failure to  
14 successfully manage our international operations and the associated risks  
15 effectively could limit the future growth of our business.

16 25. Nimble further states in its S-1 that a principal competitive factor in the intensely  
17 competitive data storage industry characterized by constant change and innovation is larger, more  
18 mature intellectual property portfolios.

19 26. Nimble similarly acknowledges in its S-1 that continued investment in research and  
20 development and intellectual property is critical to its business. According to Nimble, in the years  
21 ending January 31, 2011, 2012, and 2013 and the six months ending July 31, 2013, Nimble has spent  
22 \$4.4 million, \$7.9 million, \$16.1 million, and \$14.4 million, respectively, on research and  
23 development.

24 27. To address these problems and gain parity with its major competitor in a highly  
25 competitive industry, Nimble targeted NetApp talent and valuable confidential and non-confidential  
26 information to compete unfairly in the marketplace. Specifically, Nimble engaged in a scheme  
27 whereby it targeted and hired former NetApp employees and resellers who possess and have access  
28 to valuable, proprietary, and/or confidential NetApp business and technical information. For  
example, Daniel Weber (“Weber”), a former NetApp Senior Systems Engineer, Timothy Binning  
 (“Binning”), a former NetApp Enterprise Account Manager, and Sandhya Klute (“Klute”) a former  
 NetApp Senior Engineering Program Manager are all alleged to have taken NetApp’s proprietary  
 and/or confidential information in violation of their respective employment agreements with NetApp  
 shortly before departing for Nimble. Weber, Binning, and Klute are currently defendants in a state

1 court action pending in Santa Clara County Superior Court. *See NetApp, Inc. v. Nimble et al.*, Case  
2 No. 1:14-cv-265454, Santa Clara County Superior Court (the “State Action”).

3 28. Moreover, upon information and belief, Nimble further attempted to inhibit the  
4 growth and progress of NetApp by encouraging those departing from NetApp to Nimble to delete,  
5 and/or make otherwise unrecoverable, inaccessible, or unavailable NetApp’s confidential and  
6 proprietary information to deprive NetApp of its employee work product. Neil Glick (“Glick”), a  
7 former NetApp Technical Marketing Engineer, and Christopher Alduino (“Alduino”), a former  
8 NetApp SAN Interoperability Engineer are alleged to have done just that and are similarly  
9 defendants in the pending State Action. Nimble is the employer of each of the individual defendants  
10 named in the State Action and is itself a defendant thereto.

11 29. According to *Forbes* magazine, when Vasudevan came to Nimble in January 2011,  
12 Nimble had 40 employees. Within a year of his arrival, Nimble experienced massive growth to 230  
13 employees. Currently, approximately 15% of Nimble’s total workforce is made up of former  
14 NetApp employees, including half of its executive staff. Between July 2012 to July 2013 alone,  
15 Nimble hired approximately 55 NetApp employees, with a focus on those who had technical and  
16 sales roles at NetApp – persons who had access to NetApp’s technical and sales documents that  
17 could help Nimble quickly develop a competing product to unfairly compete with NetApp.

18 30. Upon information and belief, Nimble regularly trades on NetApp’s name by telling  
19 customers and/or prospective customers that Nimble has acquired technology teams from NetApp,  
20 many of which were employed by NetApp for a long time, implying that Nimble’s products provide  
21 quality and functionality synonymous with NetApp.

22 31. Nimble’s unlawful conduct has extraterritorial reach to Australia and other  
23 international locations as a result of its attempt to establish a global network of channel partners  
24 critical to the success of any data storage company. In order to establish sales and distribution  
25 channels faster than the ordinary lead time in a highly specialized area of technology, Nimble  
26 targeted NetApp teams in the United States and Australia to build an infrastructure it could not have  
27 done on its own in two years’ time.

28 ///

1           32.     On September 12, 2012, Nimble announced in a press release that it had opened its  
2 Asia Pacific headquarters with a highly experienced three person executive team. Two of those  
3 three people came from NetApp. Nimble boasted that this executive team was handpicked, with  
4 Peter O'Connor ("O'Connor") as its leader. O'Connor was at NetApp for six years culminating in  
5 his role as Vice President of Sales for Asia Pacific and Japan. O'Connor joined Gavin Cohen, an  
6 individual who Nimble explained in its press release brought twenty (20) years of data storage  
7 industry experience to his Nimble role, including most recently working as Director of Technology  
8 and Strategy for NetApp Asia Pacific – the most senior technical role in the region. Nimble  
9 highlighted that Cohen was responsible for developing NetApp's product and technical strategy,  
10 driving key initiatives in the region, and evangelizing NetApp's solutions. And before his important  
11 role at NetApp, Nimble pointed out that Cohen held other senior roles at NetApp's US headquarters,  
12 including Director of Product Management and Technical Marketing. Nimble's press release spent  
13 at least as much time discussing NetApp and the critical experience and knowledge O'Connor and  
14 Cohen had of NetApp's products, strategies, and the region as it did discussing what Nimble had to  
15 offer.

16           33.     Less than one year later, Nimble announced that since the Australian sales operation  
17 began in late 2012, the team had grown to 16 employees and recruited more than 30 experienced  
18 channel partners across the region. At least half of these employees came from NetApp. Nimble's  
19 growth is no coincidence. NetApp had learned that O'Connor, and other former NetApp employees  
20 who had access to confidential NetApp customer data, may have used such confidential information  
21 to solicit NetApp's customers' business at key but not publicly known times in NetApp's sales cycle  
22 with such customers. NetApp also learned that O'Connor and other former NetApp employees now  
23 employed by Nimble stated that they intended to solicit additional NetApp employees to join Nimble,  
24 and were actively engaged in an effort to do so in violation of their employment agreements with  
25 NetApp.

26           34.     Concerned over Nimble's illegal conduct, NetApp reached out to Nimble, its CEO,  
27 and O'Connor directly on or about March 15, 2013, to seek an informal resolution. Nimble, through  
28 its attorneys Fenwick & West, denied any wrongdoing and assured NetApp that O'Connor and

1 others were reminded often not to unlawfully solicit NetApp's employees or use NetApp's  
2 confidential and/or proprietary information at Nimble. At no time during these communications did  
3 Nimble or Fenwick & West state that it was acting on behalf of Nimble AUS or that O'Connor was  
4 employed by Nimble AUS. In fact, NetApp's correspondence indicated that Mr. O'Connor worked  
5 for Nimble, a point never refuted by Nimble or its attorneys at Fenwick & West. Despite Nimble's  
6 assurances, several months later, Reynolds, working at Nimble's Australian sales office under the  
7 leadership of O'Connor, illegally accessed NetApp's protected databases to, among other things,  
8 obtain and manipulate NetApp's competing product performance data to give the false impression to  
9 possible customers that Nimble's products perform better. NetApp approached Nimble again in  
10 October 2013 to resolve this dispute, which included providing Nimble with a draft complaint. Once  
11 again, Nimble did not take NetApp seriously. As a result, NetApp filed the lawsuit now pending in  
12 Federal Court.

13 **C. Reynolds Accesses NetApp's Protected Computer Systems Without Authorization**

14 35. Upon information and belief, between October 2011 and April 2013, Reynolds was  
15 employed by Thomas Duryea Consulting ("TDC"), an Australian IT infrastructure consultancy  
16 business with offices in Melbourne and Sydney, Australia.

17 36. On or about September 29, 2008, NetApp Australia Pty Limited, the Australian entity  
18 which NetApp controls, entered into a Reseller Authorization Agreement with TDC which provides,  
19 among other things, that the parties and their employees: (a) agree to hold the proprietary or  
20 confidential information of the other party in strict confidence; (b) will not copy, reproduce, or  
21 otherwise use such information for any purpose other than the provision of services under the  
22 agreement; and (c) will protect the other party's protected non-public information, including any  
23 intellectual property. These restrictions and prohibitions on the use of proprietary or confidential  
24 information were in place during the entirety of Reynolds' employment with TDC and remain in  
25 effect today.

26 37. NetApp grants or limits access to the protected systems, networks of computers, and  
27 data storage devices which contain proprietary and confidential information through the use of  
28 username and password pairs granted to NetApp employees and resellers for the purpose of selling

1 NetApp products. Reynolds was provided access to NetApp's protected computers as a result of his  
2 employment with TDC. The username and password and other security measures implemented for  
3 these protected computers is administered in California.

4 38. Reynolds took and completed a series of training courses offered by NetApp that are  
5 available to NetApp employees and approved resellers, including web-based, virtual live web casts,  
6 and in person courses such as NetApp's Accredited Storage Architect Program ("ASAP"). Many of  
7 those courses, training materials, and administration thereof are maintained in Sunnyvale, California.  
8 Even after Reynolds decided to join Nimble, and would no longer be selling NetApp products, he  
9 continued to take NetApp training courses.

10 39. Reynolds also had access to NetApp's Support Portal, which contains NetApp  
11 software and firmware downloads, product documentation, training course information, and other  
12 additional resources.

13 40. In order to resell NetApp products and services while at TDC, Reynolds had access to  
14 NetApp's Field Portal and TechNet sites, Synergy database, Support Portal, and System  
15 Performance Modeler Application database ("SPM"), which are for NetApp partners and employees,  
16 require a user login and password, and contain NetApp confidential and proprietary information.

17 41. Many of the materials provided to Reynolds during his training with NetApp – as  
18 well as the resources provided to Reynolds on the NetApp Support Portal, Field Portal, TechNet site,  
19 Synergy database, and SPM database – identify NetApp as a California corporation, with its  
20 headquarters located in Sunnyvale. The materials also explain that NetApp's databases are located  
21 in California and that the information contained therein is confidential and proprietary to NetApp.

22 42. Upon information and belief, Reynolds also was advised by TDC and/or otherwise  
23 made aware of his obligation to hold NetApp's proprietary and/or confidential information in strict  
24 confidence, and not to copy, reproduce, transfer or otherwise disclose such information to third  
25 parties or to use such information for any purpose whatsoever other than the provision of services for  
26 NetApp.

27 43. Following Reynolds' departure from TDC in April 2013, Reynolds was not  
28 authorized to access, copy, or download NetApp's computerized data. When he began working for

1 Nimble, Reynolds knew or should have known that his access was unauthorized because he was no  
 2 longer reselling NetApp products and services. To the contrary, at the time he wrongfully accessed  
 3 NetApp's data, Reynolds was working for a direct competitor (Nimble) and competing against  
 4 NetApp.

5 **D. Reynolds and Nimble Surreptitiously Obtain NetApp's Confidential and Proprietary**  
 6 **Information**

7 44. On or about May 2013, Reynolds began employment with Nimble's Australian sales  
 8 office. After beginning his employment with Nimble, Reynolds accessed NetApp's protected  
 9 computers on a variety of occasions from June 3, 2013 through August 2013, including but not  
 10 limited to the following:

- 11 • Accessed NetApp's Synergy database on six (6) occasions on or about June 4,  
 12 2013;
- 13 • Accessed NetApp's System Performance Modeler Application database once  
 14 on or about July 25, 2013 and on three (3) occasions on or about August 14,  
 15 2013;
- 16 • Accessed NetApp's Support Portal on seven (7) separate occasions between  
 17 June 3, 2013 and August 14, 2013;
- 18 • Accessed the Field Portal on three (3) separate occasions between June 2,  
 19 2013 and July 18, 2013; and
- 20 • Accessed the TechNet Site on four (4) separate occasions between July 24,  
 21 2013 and August 14, 2013.

22 45. NetApp's Synergy database, System Performance Modeler Application database,  
 23 Field Portal, TechNet Site, and Support Portal all require login credentials because they contain  
 24 confidential and proprietary information including but not limited to, NetApp's products and  
 25 services and NetApp's application framework that allows customers to build accurate and detailed  
 26 models of NetApp products and services. These systems derive independent value because they are  
 27 available only to NetApp employees, partners, and approved NetApp resellers selling products for  
 28 NetApp. Such systems – and the information contained therein – are a product of significant

1 research and development investment by NetApp and are an important competitive advantage for  
2 NetApp.

3 46. Access to and/or use of information obtained from NetApp's Synergy database is  
4 governed by an End User License Agreement ("EULA"), an advisory preceding the download of the  
5 Synergy software ("Legal Notice"), and a warning that the Synergy software is to be used only by  
6 NetApp employees and registered NetApp partners and that any use by other persons or parties is  
7 prohibited ("Download Warning"). Under the terms of the EULA, users agree that they will use the  
8 software solely as embedded in, and for execution on, NetApp equipment originally purchased from  
9 NetApp or its authorized resellers, and further agree to give NetApp the right to perform an audit of  
10 their books, records, systems, and usage associated with the software to verify compliance with the  
11 EULA. By installing and/or using the software, users indicate their acceptance of the EULA and all  
12 terms stated therein. Further, users are advised in the Download Warning that "USE OF THIS  
13 PRODUCT, INCLUDING THIS VERSION HISTORY, IS FOR NETAPP EMPLOYEES AND  
14 REGISTERED NETAPP PARTNERS. USAGE BY ANY OTHER PERSONS OR PARTIES IS  
15 PROHIBITED." In addition, the Synergy Legal Notice, which was acknowledged and agreed to by  
16 Reynolds, reads in pertinent part that the contents of the database are proprietary and unauthorized  
17 distribution may result in civil and/or criminal penalties.

18 47. Upon information and belief, at the time Reynolds downloaded NetApp's Synergy  
19 Software, he was aware of the confidential and proprietary nature of the information he was  
20 accessing, and was aware of the terms of use. And during each subsequent access to the Synergy  
21 database, Reynolds was advised that the material contained therein was NetApp's confidential and  
22 propriety information. Reynolds, like other Synergy users, received system notifications and  
23 updates indicating that the messages were being sent from NetApp in Sunnyvale, California. The  
24 Synergy user manual, which is available to all Synergy users, references NetApp in Sunnyvale,  
25 California.

26 48. As a Nimble employee, who was no longer employed by TDC, and thus no longer  
27 selling NetApp's products, Reynolds had no reason to access NetApp's restricted databases other  
28 than to use the confidential and proprietary information he obtained against NetApp – and for the

1 benefit of Nimble – in the marketplace.

2 49. Upon information and belief, Reynolds has used the confidential and proprietary  
3 information he wrongfully and illegally obtained from NetApp's protected databases while soliciting  
4 business for Nimble.

5 **FIRST CAUSE OF ACTION**

6 **Violations of Computer Fraud and Abuse Act**  
7 **18 U.S.C. §§ 1030(a)(2)(C) & (a)(4) & (a)(5)**  
8 **(Against Defendants Reynolds and Nimble)**

9 50. NetApp incorporates by reference each of the allegations in the preceding paragraphs  
10 of this Second Amended Complaint as if set forth fully herein.

11 51. Upon information and belief, if Reynolds is not an employee of Nimble, by itself or  
12 as the alter ego of Nimble AUS, then Reynolds as an employee of Nimble AUS, conspired with  
13 Nimble to commit acts which constitute violations of the Computer Fraud and Abuse Act so that  
14 Nimble could obtain a competitive edge in the marketplace through illegal access to NetApp's  
15 protected computers to access NetApp's confidential and proprietary information, valuable non-  
16 confidential training, and other materials, which constitute NetApp property. Upon information and  
17 belief, Reynolds, Nimble, and other Nimble employees, such as O'Connor, Varun Mehta, Chris  
18 Wade and Vasudevan, who all had contractual obligations to NetApp, were aware of Reynolds'  
19 ability to access NetApp's protected computers, agreed to damage NetApp by depriving it of the  
20 benefit of its agreements with Reynolds by inducing Reynolds to breach his agreements with  
21 NetApp to access its protected computers and alter or modify its data for Nimble's benefit. Upon  
22 information and belief, Reynolds and Nimble furthered the conspiracy by cooperating with each  
23 other, encouraging each other, and ratifying and adopting the acts of Reynolds and each other, and  
24 committing one or more overt acts to further the conspiracy for their own benefit including but not  
25 limited to: (a) using confidential and non-confidential data contained on NetApp's protected  
26 computers for their own purposes and not for the benefit of NetApp; (b) improperly accessing,  
27 acquiring, transmitting, and retaining NetApp's confidential and non-confidential data contained on  
28 NetApp's protected computers; (c) targeting NetApp employees and resellers who had access to  
NetApp's protected computers to provide that access to Nimble; and (d) knowing that Reynolds was

1 accessing NetApp's protected computers and doing nothing to stop his conduct.

2 52. Nimble, by itself or as the alter ego of Nimble AUS, with Reynolds acting as its agent  
3 in the course and scope of his employment and for the benefit of his employer Nimble, or its alter  
4 ego Nimble AUS, violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by  
5 intentionally accessing a computer used for interstate and foreign commerce or communication,  
6 without authorization or by exceeding authorized access to such a computer, and by obtaining  
7 information from such a protected computer. As Reynolds' employer, Nimble, by itself or as the  
8 alter ego of Nimble AUS, is vicariously and jointly liable for the unlawful acts committed by  
9 Reynolds either because Reynolds acted within the scope of his employment, because Nimble  
10 directed Reynolds to access NetApp's protected computers for its own benefit, and/or because  
11 Nimble knew or should have known what Reynolds was doing and did nothing to stop his conduct.

12 53. Reynolds and Nimble, by itself or as the alter ego of Nimble AUS, violated the  
13 Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(4) by knowingly, and with intent to defraud  
14 NetApp, accessing a protected computer without authorization, and by means of such conduct  
15 furthered the intended fraud and obtained one or more things of value, including but not limited to  
16 NetApp's software, support materials, and information about how NetApp products work.

17 54. Reynolds and Nimble, by itself or as the alter ego of Nimble AUS, violated the  
18 Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A) by knowingly causing the transmission  
19 of a program, information, code, or command, and as a result, intentionally causing damage without  
20 authorization to a protected computer owned by NetApp by among other things: (a) diminishing the  
21 value of NetApp's data by compromising its exclusivity, for which it derives value because it is not  
22 available to competitors; (b) upon information and belief, altering or modifying NetApp's  
23 performance data contained on its protected computers; and (c) upon information and belief, copying  
24 certain information from NetApp's protected computers and transferring it to a non-secure area or  
25 device.

26 55. Reynolds and Nimble, by itself or as the alter ego of Nimble AUS, violated the  
27 Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(5)(B) & (C) by intentionally accessing a  
28 protected computer without authorization, causing damage to NetApp, recklessly or without due

1 regard for their actions by among other things: (a) diminishing the value of NetApp's data by  
 2 compromising its exclusivity from which NetApp derives value because the data is not available to  
 3 competitors; (b) upon information and belief, altering or modifying NetApp's performance data  
 4 contained on its protected computers; and (c) upon information and belief, copying certain  
 5 information from NetApp's protected computers and transferring it to a non-secure area or device.

6 56. Each of the computer system or systems that Reynolds and Nimble accessed as  
 7 described above constitutes a "protected computer" within the meaning of 18 U.S.C. § 1030(e)(2).

8 57. As a result of Reynolds' and Nimble's conduct, by itself or as the alter ego of Nimble  
 9 AUS, NetApp has suffered damage including, without limitation, harm to the integrity of its data,  
 10 programs, and computer system as well as losses related to such items as investigation costs  
 11 including attorneys' fees and internal NetApp time, in an amount to be proved at trial, but, in any  
 12 event, in an amount well over \$5,000.00, the minimum statutory amount, aggregated over a one-year  
 13 period.

14 58. Reynolds' and Nimble's, by itself or its alter ego Nimble AUS, unlawful access to  
 15 and theft from NetApp's computers also has caused NetApp irreparable injury. Unless restrained  
 16 and enjoined, Nimble and Reynolds will continue to use the wrongfully and illegally obtained  
 17 NetApp confidential and proprietary information against NetApp in the marketplace. NetApp's  
 18 remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling  
 19 NetApp to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

## 20 **SECOND CAUSE OF ACTION**

### 21 **Trespass to Chattels** 22 **(Against Defendants Reynolds and Nimble)**

23 59. NetApp incorporates by reference each of the allegations in the preceding paragraphs  
 24 of this Second Amended Complaint as if set forth fully herein.

25 60. NetApp's password protected computer systems are NetApp property and are  
 26 repositories of valuable confidential and/or proprietary information that are essential to NetApp's  
 27 technical support services.

28 61. NetApp's password protected computer systems are also repositories of valuable

1 non-confidential information such as certain training materials and company information that  
2 NetApp has invested substantial time and money preparing and to which Reynolds and Nimble, by  
3 itself or as the alter ego of Nimble AUS, have benefited by not having to spend the time and  
4 resources to scour publicly available NetApp information and digest that information so that it is  
5 readily available all in one place. NetApp retains a property right in these materials because, among  
6 other reasons, they are corporate employee work product using NetApp resources to develop and are  
7 considered copyrighted material.

8 62. Nimble, by itself or as the alter ego of Nimble AUS, through Reynolds' access to and  
9 downloading from NetApp's protected computer systems, as described above, intentionally and  
10 without authorization interfered with NetApp's possessory interest in NetApp's computer systems  
11 by accessing NetApp's protected computers at least twenty (23) three times after joining Nimble.

12 63. Reynolds' bad acts were committed while employed by Nimble, by itself or as the  
13 alter ego of Nimble AUS, within the scope of his employment. As Reynolds' employer and the alter  
14 ego of Nimble AUS, Nimble is vicariously and jointly liable for the unlawful acts committed by  
15 Reynolds.

16 64. Reynolds' and Nimble's, by itself or as the alter ego of Nimble AUS, unauthorized  
17 use proximately resulted in damage to NetApp.

18 65. The damage to NetApp's property includes, but is not limited to, the diminution of  
19 value of these proprietary resources by among other reasons: (a) diminishing the value of NetApp's  
20 data by compromising its exclusivity from which NetApp derives value because the data is not  
21 available to competitors; (b) upon information and belief, altering or modifying NetApp's  
22 performance data contained on its protected computers; and (c) upon information and belief, copying  
23 certain information from NetApp's protected computers and transferring it to a non-secure area or  
24 device.

25 66. NetApp is entitled to compensatory damages, injunctive relief, and such other relief  
26 as the Court may deem appropriate, with such sums to be determined at trial.

27 ///

28 ///

**THIRD CAUSE OF ACTION**

**Breach of Contract  
(Against Defendant Reynolds)**

67. NetApp incorporates by reference each of the allegations in the preceding paragraphs of this Second Amended Complaint as though fully set forth herein.

68. Reynolds downloaded the Synergy software and, in doing so, accepted the terms of the applicable Use Restrictions.

69. NetApp's offer to Reynolds of a non-exclusive, limited, royalty-free license, to install and use the Synergy software subject to the Use Restrictions, and Reynolds' acceptance of these terms as evidenced by his downloading of the Synergy software, constitutes a valid and enforceable contract under California law.

70. Reynolds breached the Use Restrictions by engaging in the unauthorized reproduction and/or distribution of the Synergy software program, data, and portions thereof. Upon information and belief, Reynolds used the Synergy software and accessed NetApp's Synergy database and used the confidential and proprietary information contained therein against NetApp – and for the benefit of Nimble to compete unfairly in the marketplace.

71. As a direct and proximate cause of Reynolds' breach of the Use Restriction, NetApp has suffered economic injury and damages in an amount to be proven at trial.

72. By downloading the Synergy software, Reynolds also agreed that breach of the Use Restrictions, and specifically the EULA, would "cause irreparable injury to NetApp for which monetary damages would not be an adequate remedy" and further agreed that NetApp shall be entitled to seek equitable relief in addition to any remedies it may have under the EULA or at law. Accordingly, NetApp seeks an order requiring that Reynolds give NetApp access to his books, records, systems, and usage associated with the Software to verify the extent and nature of Reynolds' non-compliance with the Use Restrictions.

**FOURTH CAUSE OF ACTION**

**Unfair Competition  
California Business and Professions Code § 17200, *et seq.*  
(Against Defendants Reynolds and Nimble)**

73. NetApp incorporates by reference each of the allegations in the preceding paragraphs

1 of this Second Amended Complaint as if fully set forth herein.

2 74. NetApp is a “person” within the meaning of California Business & Professions Code  
3 Section 17201.

4 75. As alleged herein, Reynolds and Nimble, by itself or as the alter ego of Nimble AUS,  
5 have engaged in unlawful business acts or practices by committing some or all illegal acts and  
6 practices alleged herein and above including: (a) illegal access to NetApp’s protected databases,  
7 which constitutes NetApp property, in violation of the Computer Fraud and Abuse Act; (b) trespass  
8 to chattel by illegally accessing NetApp’s protected databases, which constitutes NetApp property;  
9 (c) trading on NetApp’s name in violation of the spirit of state and federal trademark laws; and,  
10 (d) in the case of Reynolds only, breach of contract, for among other reasons his unauthorized use,  
11 reproduction and/or distribution of NetApp’s software, which constitutes NetApp property, for the  
12 benefit of Nimble and in violation of the spirit of state and federal copyright laws, all in an effort to  
13 gain an unfair competitive advantage over NetApp and to deceive consumers.

14 76. As alleged herein, Nimble’s conduct, by itself or as the alter ego of Nimble AUS,  
15 constitutes “unfair” business practices by at least: (a) targeting teams of NetApp employees and  
16 resellers to open an Australian sales office and to transport necessary infrastructure from NetApp to  
17 Nimble in violation of their contractual obligation to NetApp so that Nimble could expand its sales  
18 market quicker and not have to invest substantial resources in developing its sales and distribution  
19 channels; (b) trading on NetApp’s name by hiring teams formerly employed by NetApp in Australia  
20 in order to compete unfairly in the marketplace and deceive consumers into thinking that Nimble is  
21 an innovator and can provide products that are “just like NetApp but cheaper;” (c) encouraging  
22 Nimble employees who work with Reynolds to delete NetApp information before their departure in  
23 an attempt to further frustrate NetApp’s ability to compete; (d) encouraging Reynolds and others to  
24 manipulate NetApp data, which constitutes NetApp property, to give the false impression that  
25 NetApp’s competing products do not perform as well as Nimble products; and (e) encouraging its  
26 employees who work in its Australian sales office, including Reynolds, to use their knowledge of  
27 NetApp’s products to access a compilation of non-confidential copyright protected NetApp training  
28 and other materials on NetApp’s protected computers, which constitute NetApp property that

1 NetApp has invested substantial time and money preparing, and to which Nimble has benefited by:  
2 (i) not having to spend the time and resources to scour publicly available NetApp information; and  
3 (ii) digest that information so that it is readily available all in one place. All of Nimble's conduct, by  
4 itself or as the alter ego of Nimble AUS, as described above, ultimately threatens or harms the  
5 consumer of NetApp products and competition in the data storage industry.

6 77. As alleged herein and above, Reynolds' conduct constitutes "unfair" business  
7 practices by: (a) manipulating NetApp's copyright protected data, which constitutes NetApp's  
8 property, to give the false impression that NetApp's competing products do not perform as well as  
9 Nimble's products; (b) using his knowledge of NetApp's products through access to a compilation  
10 of non-confidential copyright protected NetApp training and other materials, which constitute  
11 NetApp property, to assist him in unfairly competing against NetApp with materials that NetApp  
12 has invested substantial time and money preparing and to which Reynolds has benefited by: (i) not  
13 having to spend the time and resources to scour publicly available NetApp information; and (ii)  
14 digest that information so that it is readily available all in one place; (c) unauthorized use,  
15 reproduction and/or distribution of NetApp's copyright protected Synergy software, which  
16 constitutes NetApp property, to access NetApp protected computers for the improper purpose of  
17 manipulating NetApp's performance data to give the false impression that NetApp's competing  
18 products do not perform as well as Nimble's products; and (d) accessing NetApp's protected  
19 databases and continuing to take NetApp training courses after he knew he was going to work for  
20 Nimble. All of Reynolds' conduct, as described above, ultimately threatens or harms the consumer  
21 of NetApp products and competition in the data storage industry.

22 78. By reason of, and as a direct and proximate result of Reynolds' and Nimble's, by  
23 itself or as the alter ego of Nimble AUS, unfair and unlawful practices and conduct, as described  
24 herein, NetApp has suffered and will continue to suffer, financial injury to its business and property  
25 in an amount to be determined at trial.

26 79. A permanent and mandatory injunction against Reynolds and Nimble, by itself or as  
27 the alter ego of Nimble AUS, collectively and severally, is necessary to stop these ongoing unlawful  
28 and unfair business practices.

80. NetApp is entitled to disgorgement and/or restoration of any and all revenues, earnings, profits, compensation, and benefits Nimble obtained by itself or as the alter ego of Nimble AUS, in violation of California Business & Professions Code § 17200 *et seq.*, including, but not limited to, returning the value of the stolen property itself and any revenue earned from it. NetApp also is entitled to injunctive relief, in that Nimble should be enjoined from further unlawful, unfair, and deceptive business practices, and Reynolds and Nimble should be further ordered to return all materials taken from NetApp, and all copies of such, in their possession, custody, or control.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for judgment as follows:

1. For entry of judgment against Reynolds and Nimble, by itself or as the alter ego of Nimble AUS, on all Claims for Relief;
2. For an injunction preliminarily and permanently prohibiting Reynolds and Nimble and their officers, agents, servants, employees, and all persons acting in concert with it and/or them, from directly or indirectly:
  - a. Acquiring, using, possessing, disclosing, conveying, or communicating to any person any of Plaintiff's confidential or other valuable proprietary information;
  - b. Manufacturing, producing, offering for sale, selling, or conveying to any person any products, systems or services produced, manufactured, or marketed using Plaintiff's confidential or other valuable proprietary information;
3. For an order requiring that Reynolds give Plaintiff access to his laptops, hard drives, external storage media, and all other electronic media where Plaintiff's Confidential or other valuable proprietary information may be stored;
4. For an order requiring that Nimble give Plaintiff access to its computer systems and servers to verify the extent and nature of Plaintiff's confidential or other valuable proprietary information stored therein;
5. For compensatory damages in an amount according to proof;

6. For an award of punitive damages; and

7. For such other relief as the Court deems just and proper.

DUANE MORRIS LLP

Dated: June 2, 2014

By: /s/ Karineh Khachatourian

Karineh Khachatourian

Patrick S. Salceda

David T. Xue

Attorneys for Plaintiff

NETAPP, INC.

**DEMAND FOR JURY TRIAL**

Pursuant to Federal Rule of Civil Procedure 38(b), NetApp, Inc. hereby demands trial by jury as to all issues in this action triable by a jury.

DUANE MORRIS LLP

Dated: June 2, 2014

By: /s/ Karineh Khachatourian

Karineh Khachatourian

Patrick S. Salceda

David T. Xue

Attorneys for Plaintiff

NETAPP, INC.

DM2\4954711.1